UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/432,007	11/01/1999	AKIHISA KAWASAKI	MAT-V07838	9503

7590 03/11/2004

LAWRENCE E ASHERY
RATNER & PRESTIA SUITE 301
ONE WESTLAKES BERWYN
PO BOX 980
VALLEY FORGE, PA 194820980

EXAMINER	
ZIA, SYED	

ART UNIT	PAPER NUMBER
2131	6

DATE MAILED: 03/11/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/432,007	**Applicant(s)** KAWASAKI, AKIHISA	
	Examiner Syed Zia	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 November 1999*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 4 .

4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: .

DETAILED ACTION

Information Disclosure Statement

1. The information disclosure statement filed on February 05, 2004 (Paper N0. 5) fails to comply with 37 CFR 1.98(a)(3) because it does not include a concise explanation of the relevance, as it is presently understood by the individual designated in 37 CFR 1.56(c) most knowledgeable about the content of the information, of each patent listed that is not in the English language. It has been placed in the application file, but the information referred to therein has not been considered.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

2. Claims 1-28 are rejected under 35 U.S.C. 102(e) as being anticipated by Chaum et al. U. S. Patent (5,485,520).

3. Regarding Claim 1 Chaum teaches and describes an equipment authentication and cryptographic communication system, comprising: user-end equipment, system-end equipment, and a key center for administrating authentication of equipment in said system (Fig.1), wherein;

- said user-end equipment provided with individual user-end equipment information issued by said key center and individual user-end equipment secret information corresponding to said individual user-end equipment's information, and said use-end equipment transmits said individual user-end equipment information to said system-end equipment (col.6 line 65 to col.7 line 65);

- said system-end equipment receives said individual user-end equipment information from said user-end equipment, reproduces said individual user-end equipment secret information from said received individual user-end equipment information, and authenticates said user-end equipment by confirming that said user-end equipment legitimately has said individual user-end equipment secret information by using a challenge response utilizing a common key cryptographic algorithm (col.7 line 38 to col.8 line 25); and

- said user-end equipment and said system-end equipment execute a cryptographic communication with each other using said individual user-end equipment secret information (col.9 line 36 to line 48).

4. Regarding Claim 12 Chaum teaches and describes an equipment authentication and cryptographic communication system, comprising: user-end equipment, system-end equipment, and a key center for administrating authentication of equipment in said system, wherein;

- said key center is provided with a first system converter for generating user-end equipment secret information from user-end equipment information (col.6 line 65 to col.7 line 7);

- said user-end equipment is provided with a first storage unit for storing said user-end equipment information provided by said key center, a second storage unit for storing said user-end equipment secret information, a first encryption unit, and a first decryption unit (col.7 line 37 to col.8 line 5, and col.10 line 66 to col.11 line 25); and

- said system-end equipment is provided with a second system converter for generating said user-end equipment secret information by a system conversion of said user-end equipment information received from said user-end equipment, a second encryption unit, and a second decryption unit, and wherein said user-end equipment and said system-end equipment share and utilize said user-end equipment secret information as a common key for encryption and decryption in said first encryption unit and said first decryption unit in said user-end equipment, and said second encryption unit and said second decryption unit in said system-end equipment (col.9 line 25 to line 48).

5. Regarding Claim 14 Chaum teaches and describes a method of equipment authentication and cryptographic communication for an equipment authentication and cryptographic communication system including user-end equipment, system-end equipment, and a key center for administrating authentication of equipment in said system, said method comprising the steps of:

- generating user-end equipment secret information from user-end equipment information in said key center (col.6 line 65 to col.7 line 7);

- receiving said user-end equipment information and said user-end equipment secret information in said user-end equipment from said key center (col.7 line 37 to col.8 line 5);

- receiving said user-end equipment information from said user-end equipment, and generating said user-end equipment secret information from said user-end equipment information received in said system-end equipment, and using said user-end equipment secret information as a common key for encryption and decryption in both of said user-end equipment and said system-end equipment (col.9 line 25 to line 48, and col.10 line 66 to col.11 line 25).

6. Regarding Claim 17 Chaum teaches and describes a cryptographic communication system comprising: an IC card, authentication equipment for authenticating said IC card, and intermediary equipment between said IC card and said authentication equipment, wherein;

- said IC card includes a first storage unit for storing a secret key particular to said IC card, a second storage unit for storing a certificate of individual IC card key data for generating said secret key, a third storage unit for storing an IC card ID data, and an encryption unit for generating an encrypted data representing response data by encrypting challenge data received from said authentication equipment using said secret key (col.3 line 10 to line 45, col.5 line 54 to col.6 line 19, and col.7 line 37 to line 65); and

- said authentication equipment includes a means for producing said secret key particular to said IC card from said certificate of individual IC card key data received, a first decryption unit for reproducing said response data by decrypting said encrypted data received from said IC card using said produced secret key, and a first matching determination unit for determining if reproduced response data matches said challenge data transmitted by said authentication equipment (col. 5 line 54 to col.6 line 19, and col.8 line 36 to col.54).

7. Regarding Claim 21 Chaum teaches and describes an electronic toll collection ("ETC") authentication system including an IC card, roadside equipment, and central processing equipment, comprising:

- said IC card including an encryption means for receiving a challenge data generated by roadside equipment, as said IC card passes said roadside equipment, and for encrypting said challenge data using a secret key, an encrypted data storage means for storing data encrypted by said encryption means, a response data transmission means for transmitting IC card ID data and a certificate of individual IC card key, together with said encrypted data stored in said encrypted data storage means, as response data to said roadside equipment (col.3 line 10 to line 45, col.5 line 54 to col.6 line 19, and col.7 line 37 to line 65);

- said roadside equipment including a dividing means for dividing said transmitted response data, a second decryption means for decrypting said certificate of individual IC card key data divided by said dividing means, using a validation key; a first matching determination means for making a matching determination of said IC card ID produced as a result of decryption with another IC card ID provided by said dividing means; a first decryption means for producing response data by decrypting an encrypted data provided by said dividing means; and a challenge data transmission means for transmitting said challenge data to said IC card (col. 5 line 54 to col.6 line 19, and col.8 line 36 to col.54) ; and

- said central processing equipment including challenge data storage means for storing said challenge data generated by said roadside equipment; and a second matching determination means for receiving said response data decrypted by said first decryption means, and executing a matching determination of said response data with said challenge data stored in said challenge data storage means, said ETC authentication system providing authentication of said IC card ID by said roadside equipment by authenticating signature information received with said IC card ID, and said central processing equipment providing a matching determination of said response data encrypted by said IC card and decrypted by said roadside equipment (col.3 line 10 to line 45, and col.7 line 37 to line 65).

8. Regarding Claim 22 Chaum teaches and describes an electronic toll collection ("ETC") authentication method comprising the steps of:

- encrypting challenge data using a secret key in an IC card, said challenge data being generated by roadside equipment and transmitted to said IC card when said IC card passes by said roadside equipment, storing said encrypted data, transmitting an IC card ID data and a certificate of individual IC card key data, in addition to said stored encrypted data, as response data to said roadside equipment (col.3 line 10 to line 45, col.5 line 54 to col.6 line 19, and col.7 line 37 to line 65);

- dividing said response data received by said roadside equipment, decrypting said certificate of individual IC card key data, provided by the dividing step, using a validation key, carrying out a matching determination of an IC card ID provided in the decrypting step with another IC card ID provided in the dividing step, providing a response data by decrypting said encrypted data provided in the dividing step (col. 5 line 54 to col.6 line 19, and col.8 line 36 to col.54); and

- carrying out in said central processing equipment a matching determination of said response data decrypted by said roadside equipment with said challenge data, said ETC authentication method providing authentication of said IC card ID by said roadside equipment by authenticating signature information received with said IC card ID, and said central processing equipment providing a matching determination of said response data encrypted by said IC card and decrypted by said roadside equipment (col.3 line 10 to line 45, and col.7 line 37 to line 65).

9. Regarding Claim 23 Chaum teaches and describes an electronic toll collection ("ETC") authentication system comprising:

- first roadside equipment including challenge data and time generator I storage means for generating and storing challenge data and time information, and transmitting said challenge data and time information to an IC card, said IC card including an ID transmission means for transmitting an IC card ID before said IC card passes said first roadside equipment; an encryption means for receiving said challenge data and said time information generated by said first roadside equipment, as said IC card passes said first roadside equipment, and encrypting received data using a secret key; a response data transmission means for transmitting an IC card ID data and a certificate of individual IC card key data, together with said encrypted data as a response data to a second roadside equipment (col.3 line 10 to line 45, col.5 line 54 to col.6 line 19, and col.7 line 37 to line 65);

- said second roadside equipment including a first dividing means for dividing said response data, a second decryption means for decrypting said certificate of individual IC card key data divided by said first dividing means, using a validation key, a first matching determination means for providing a matching determination of an IC card ID produced as a result of decryption with another IC card ID provided by said first dividing means; and a first decryption means for producing a response data by decrypting an encrypted data obtained from said first dividing means (col. 5 line 54 to col.6 line 19, and col.8 line 36 to col.54); and

- central processing equipment including a second dividing means for dividing said challenge data and said IC card ID generated by said first roadside equipment; a third dividing means for dividing said response data and said IC card ID decrypted by said second roadside equipment; and a second matching determination means for making a matching determination of said challenge data obtained by said second dividing means and said response data provided by said third dividing means, said ETC authentication system ,providing authentication of said IC card ID by said second roadside equipment by authenticating signature information received with said IC card ID, and said central processing equipment providing the matching determination of said response data encrypted by said IC card and decrypted by said second roadside equipment (col.3 line 10 to line 45, and col.7 line 37 to line 65).

10. Regarding Claim 25 Chaum teaches and describes an electronic toll collection ("ETC") authentication method comprising the steps of:

- receiving a card ID from an IC card before said IC card passes first roadside equipment, encrypting challenge data and time information using a secret key, said challenge data and tune information being generated by first roadside equipment and transmitted to said IC card when said IC card passes said first roadside equipment, transmitting IC card ID data and a certificate of individual IC card key data, in addition to said encrypted data, as a response data to second roadside equipment (col.3 line 10 to line 45, col.5 line 54 to col.6 line 19, and col.7 line 37 to line 65);

- dividing said transmitted response data in said second roadside equipment, decrypting said certificate of individual IC card key data provided in the dividing step using a validation key, carrying out a matching determination of an IC card ID provided in the decryption step with another IC card ID provided in the dividing step, providing a response data by decrypting said encrypted data provided in the dividing step (col. 5 line 54 to col.6 line 19, and col.8 line 36 to col.54);

- carrying out in central processing equipment a matching determination of said challenge data provided from said first roadside equipment and said response data decrypted in said second roadside equipment, said ETC authentication method providing authentication of said IC card ID by said second roadside equipment by authenticating signature information received with said IC card ID, and said central processing equipment providing the matching determination of said response data encrypted by said IC card and decrypted by said second roadside equipment (col.3 line 10 to line 45, and col.7 line 37 to line 65).

11. Regarding Claim 27 Chaum teaches and describes an electronic toll collection ("ETC") authentication system comprising:

- a first roadside equipment including a challenge data generation means for generating a challenge data, and transmitting said challenge data to an IC card, said IC card including an ID transmission means for transmitting an IC card ID before said IC card passes said first roadside equipment, an encryption means for receiving said challenge data generated by said first roadside equipment, as said IC card passes said first roadside equipment, and encrypting said challenge data using a secret key; and a response data transmission means for transmitting an IC card ID data and a certificate of individual IC card key data, together with said encrypted data as response data to second roadside equipment (col.3 line 10 to line 45, col.5 line 54 to col.6 line 19, and col.7 line 37 to line 65);

- said second roadside equipment including a first dividing means for dividing said response data; a decryption means for decrypting said certificate of individual IC card key data divided by said first dividing means, using a validation key; a first matching determination means for providing a matching determination of said IC card ID produced as a result of decryption with another IC card ID provided by said first dividing means; and a first decryption means for decrypting an encrypted data provided by said first dividing means to obtain response data (col. 5 line 54 to col.6 line 19, and col.8 line 36 to col.54);

- central processing equipment including a second dividing means for dividing said challenge data and said IC card ID generated in said first roadside equipment, a third dividing means for dividing said response data decrypted in said second roadside equipment and said IC card ID; and a second matching determination means for providing a matching determination of said challenge data obtained in said second dividing means and said response data obtained in said third dividing means, said ETC authentication system providing authentication of said IC card ID by said second roadside equipment by authenticating signature information received with said 1C card ID, and said central processing equipment providing the matching determination of said response data encrypted by said 1C card and decrypted by said second roadside equipment (col.3 line 10 to line 45, and col.7 line 37 to line 65).

12. Regarding Claim 28 Chaum teaches and describes an electronic toll collection ("ETC") authentication method comprising the steps of:

- receiving a card ID from an IC card before said IC card passes by first roadside equipment, encrypting a challenge data using a secret key, said challenge data being generated by said first roadside equipment and transmitted to said IC card when said IC card passes said first roadside equipment, transmitting each individual data of said IC card ID and a certificate of individual IC card key, in addition to said challenge data encrypted in the encryption step, as response data to second roadside equipment (col.3 line 10 to line 45, col.5 line 54 to col.6 line 19, and col.7 line 37 to line 65);

- dividing said response data transmitted in the transmission step by said second roadside equipment, decrypting said certificate of individual IC card key data divided in the dividing step, using a validation key, carrying out a matching determination of said IC card ID produced as a result of decryption with another IC card ID provided by the dividing step, producing a response data by decrypting said encrypted data provided by the dividing step (col. 5 line 54 to col.6 line 19, and col.8 line 36 to col.54); and

- executing in central processing equipment a matching determination of said challenge data provided by said first roadside equipment and said response data decrypted by said second roadside equipment, said ETC authentication method providing authentication of said IC card ID by said second roadside equipment by authenticating signature information received said IC card ID, and said central processing equipment providing the matching determination of said response data encrypted by said IC card and decrypted by said second roadside equipment (col.3 line 10 to line 45, and col.7 line 37 to line 65).

13. Claim 2 is rejected applied as above rejecting Claim 1. Furthermore, Chaum teaches and describes equipment authentication and cryptographic communication system wherein:

said system-end equipment is provided with system-end equipment secret information, which is identical to that possessed by said key center, and produces individual user-end equipment secret information from said individual user-end equipment information using said system-end equipment secret information; and said user-end equipment authenticates said system-end equipment by confirming that said system-end equipment has said individual user-end equipment secret information by a challenge response utilizing said common key cryptographic algorithm (col.15 line 65 to col.16 line 65).

14. Claim 3 is rejected applied as above rejecting Claim 1. Furthermore, Chaum teaches and describes equipment authentication and cryptographic communication system wherein:

- said system-end equipment is provided with a secret-key cryptographic algorithm, and reproduces said individual user-end equipment secret information by a system conversion of said individual user-end equipment information using a secret key (col.16 line 14 to col.16 line 65).

15. Claim 4 is rejected applied as above rejecting Claim 1. Furthermore, Chaum teaches and describes equipment authentication and cryptographic communication system, wherein:

- said system-end equipment and said user-end equipment are both provided with common secret information shared there between by exchanging individually held secret information (col.16 line 14 to col.16 line 65).

16. Claim 5 is rejected applied as above rejecting Claim 1. Furthermore, Chaum teaches and describes equipment authentication and cryptographic communication system wherein:

- said system-end equipment and said user-end equipment exchange with each other individually held secret information, and generate new secret information by combining said individually held secret information and said secret information exchanged there between according to a predetermined procedure (Col.15 line 22 to col.16 line 65).

17. Claim 6 is rejected applied as above rejecting Claim 1. Furthermore, Chaum teaches and describes equipment authentication and cryptographic communication system, wherein:

- said system-end equipment and said user-end equipment use said individual user-end equipment secret information for encrypting said new secret information, which is provided by combining said information and said exchanged information (col.16 line 32 to line 52).

18. Claim 7 is rejected applied as above rejecting Claim 1. Furthermore, Chaum teaches and describes equipment authentication and cryptographic communication system, wherein

- said system-end equipment and said user-end equipment individually generate random digits, exchange said generated random digits with each other, and share the same secret information particular to said system-end equipment and said user-end equipment by combining said generated random digits and said exchanged random digits according to a predetermined procedure (col.22 line 18 to line 58).

19. Claim 8 is rejected applied as above rejecting Claim 1. Furthermore, Chaum teaches and describes equipment authentication and cryptographic communication system, wherein

- said system-end equipment and said user-end equipment individually generate random digits, combine said random digits with their own information particular to each of said system-end equipment and said user-end equipment according to a predetermined procedure, generate encrypted data by encrypting the combined information using said individual user- end equipment secret information, exchange said encrypted data with each other, generate decrypted data by decrypting said exchanged encrypted data using said individual user-end equipment's secret information, and reproduce each of said mutually exchanged random digits by dividing the combination of said decrypted data according to a predetermined procedure (col.22 line 59 to col.24 line 56).

20. Claim 9 is rejected applied as above rejecting Claim 1. Furthermore, Chaum teaches and describes equipment authentication and cryptographic communication system wherein:

- said system-end equipment and said user-end equipment individually generate and store random digits, exchange said random digits with each other, combine said exchanged random digits with said individually generated and stored random digits according to a predetermined procedure, generate encrypted data by encrypting said combined information using said individual user-end equipment secret information, exchange said encrypted data with each other, generate decrypted data by decrypting said exchanged encrypted data using said individual user-end equipment secret information, and reproduce each of said mutually exchanged random digits by dividing the combination of said decrypted data according to a predetermined procedure (col.22 line 18 to col.24 line 56).

21. Claim 10 is rejected applied as above rejecting Claim 1. Furthermore, Chaum teaches and describes equipment authentication and cryptographic communication system, wherein said system-end equipment and said user- end equipment individually execute matching determinations by comparing said mutually exchanged random digits, which are produced by dividing the combination of said decrypted data according to the predetermined procedure, with said individually generated and stored random digits (col.23 line 16 tocol.24 line 65).

22. Claim 11 is rejected applied as above rejecting Claim 1. Furthermore, Chaum teaches and describes equipment authentication and cryptographic communication system, wherein

- said system-end equipment and said user-end equipment produce and store the same data by combining said exchanged and received random digits and said individually generated and stored random digits according to the predetermined procedure, and mutually share said data as a common key particular to both said system-end equipment and said user-end equipment, if said matching determination produces a positive result (co.23 line 16 to col.24 line 65, and col.26 line 37 to line 56).

23. Claim 13 is rejected applied as above rejecting Claim 1. Furthermore, Chaum teaches and describes equipment authentication and cryptographic communication system, wherein:

- said user-end equipment further comprises a first random digit generator for generating a random digit, a second random digit generator for generating a random digit, a first combiner for combining a pair of random digit data according to a predetermined procedure, a first divider for dividing a combined pair of random digit data to reproduce original random digits prior to combining, a first common key generator for combining a pair of random digit data according to a predetermined procedure, ;and a first matching determination unit for determining if two random digit data match each other (col.16 line 32 to line 52, and col.26 line 37 to line 56); and

- said system-end equipment further comprises a third random digit generator for generating a random digit, a fourth random digit generator for generating another random digit, a second combiner for combining a pair of random digit data according to a predetermined procedure, a second divider for dividing a combined pair of random digit data to reproduce original random digits prior to combining, a second common key generator for combining a pair of random digit data according to a predetermined procedure, and a second matching determination unit for determining if two random digit data match each other (col.27 line 18 to line 58, and col.26 line 37 to line 56).

24. Claim 15 is rejected applied as above rejecting Claim 1. Furthermore, Chaum teaches and describes method of equipment authentication and cryptographic communication further comprising the steps of:

- generating a first random digit in said user-end equipment, and transmitting said first random digit to said system-end equipment, generating a second random digit in said system-end equipment, combining said second random digit and said first random digit received from said user-end equipment, encrypting combined data of said second random digit and said first random digit using said common key, and transmitting said encrypted data to said user-end equipment, decrypting said encrypted data received in said user-end equipment using said common key, and reproducing said first random digit and said second random digit by dividing decrypted data of said encrypted data received in said user-end equipment, determining in said user-end equipment if said first random digit reproduced in the preceding decryption step matches with another first random digit generated therein, generating a third random digit in said user-end equipment, combining said third random digit and said second random digit reproduced in the decryption step, encrypting combined data of said third random digit and said second random digit using said common key, and transmitting encrypted data of said combined data to said system-end equipment, generating a fourth random digit in said system-end equipment, and transmitting said fourth random digit to said user-end equipment, and combining said fourth random digit received in said user-end equipment from said system-end equipment and said third random digit generated therein, encrypting combined data of said fourth random digit and said third random digit using said common key, and transmitting encrypted data of said combine data to said system-end equipment (col.16 line 32 to line 52, col.22 line 18 to line 58, col.23 line 16 to col.24 line 65, and col.26 line 37 to line 56);

- decrypting said encrypted data received in said system-end equipment using said common key, and reproducing said third random digit and said fourth random digit by dividing decrypted data of said encrypted data received in said system-end equipment, and determining in said system-end equipment if said fourth random digit reproduced in the preceding decryption step matches with another fourth random digit generated therein (col.22 line 18 to line 58, and col.26 line 37 to line 56).

25. Claim 16 is rejected applied as above rejecting Claim 1. Furthermore, Chaum teaches and describes a method of equipment authentication and cryptographic communication further comprising the steps of:

- producing data in said system-end equipment for use as a common key for cryptographic communication by combining said second random digit generated therein with said third random digit reproduced by decryption; and producing data in said user-end equipment for use as a common key for cryptographic communication by combining said third random digit generated therein and said second random digit reproduced by decryption (col.23 line 16 to col.24 to line 65, and col.26 line 37 to line 56).

26. Claim 18 is rejected applied as above rejecting Claim 1. Furthermore, Chaum teaches and describes a cryptographic communication system according to claim 17 wherein:

- said IC card further includes a receiver for receiving said challenge data generated by said authentication equipment and transmitted via said intermediary equipment, and a response data transmitter for transmitting said encrypted data representing response data, said IC card ID data, and said certificate of individual IC card key data to said authentication equipment via said intermediary equipment, and said means for producing said secret key in said authentication equipment includes a storage unit for storing a validation key, a second decryption unit for producing an IC card ID and a secret key by decrypting said certificate of individual IC card key data received from said IC card, using said validation key (col.3 line 10 line 45, col.5 line 54 to col.6 line 19, and col.7 line 37 to line 65); and
- said authentication equipment further includes a challenge data generator / storage unit for generating and storing said challenge data, and a second matching determination unit for determining if said response data decrypted by said first decryption unit matches with said challenge data stored in said challenge data generator / storage unit (col.22 line 18 to line 58, and col.26 line 37 to line 56).

27. Claim 19 is rejected applied as above rejecting Claim 1. Furthermore, Chaum teaches and describes a cryptographic communication system wherein:

- said IC card further includes a combiner for generating combined data by combining said IC card ID data, said certificate of individual IC card key data, and said encrypted data, and transmitting said combined data to said authentication equipment (col.3 line 10 to line 45); and

- said authentication equipment further includes a first divider for dividing said combined data received from said IC card into said IC card ID data, said certificate of individual IC card key data, and said encrypted data, and a second divider for dividing data decrypted by said second decryption unit into said IC card ID and said secret key (col.16 line 14 to line 65).

28. Claim 20 is rejected applied as above rejecting Claim 1. Furthermore, Chaum teaches and describes a cryptographic communication system wherein:

- said authentication equipment further includes a first combiner for combining said challenge data stored in said challenge data generator / storage unit and said IC card ID data produced by said second divider, a third divider for producing said challenge data from data combined by said first combiner, a second combiner for combining said response data decrypted by said first decryption unit and said IC card ID data produced by said second divider, and a fourth divider for producing said response data from data combined by said second combiner (col.16 line 32 to line 52, and col.26 line 37 to line 56).

29. Claim 24 is rejected applied as above rejecting Claim 1. Furthermore, Chaum teaches and describes a ETC authentication system, wherein:

- said second roadside equipment further comprises another decryption means for decrypting said encrypted data provided by said first dividing means, using a secret key reproduced by said second decryption means; and a validation means for providing time information, at which said IC card passed said first roadside equipment, from a decrypted result of said another decryption means, and for confirming if a difference between said time information and present time is within a predetermined time period (col.3 line 10 to line 45, and col.26 line 37 to line 65).

30. Claim 26 is rejected applied as above rejecting Claim 1. Furthermore, Chaum teaches and describes a ETC authentication method further comprising the steps of:

- decrypting said encrypted data provided by the dividing step, using a secret key reproduced in said decryption step; and providing time information, at which said IC card passed said first roadside equipment, as a result of the decryption step, and confirming if a difference between said time information and present time is within a predetermined time (col.3 line 10 to line 45, col.26 line 37 to line 65, and col.12 line 57 to col.13 line 28).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed Zia whose telephone number is 703-305-3881. The examiner can normally be reached on Monday - Friday 9:00 AM to 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

sz
March 6, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100